Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1325 06/24/11

~ Need Harsher Penalties ~ People Are Talking! ~ National Cyber Range!
~ DuckDuckGo Alternative ~ The .whatever Address! ~ User Online Shields!
~ Firefox 5 Auto-Updates ~ Snow Leopard Update! ~ "Twins" Drop Lawsuit!

~ Penny Auctions Are Not ~ Site Dumps Ugly People ~ Project Featherweight!

-* FBI Targets Scareware Rings! *-
-* China: No Cyber Warfare with U.S.! *-
-* Hackers On Publicity-Seeking Attack Spree! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Welcome home, Whitey!! It appears it's time to "face the music" after all these years! Being a New Englander all my life, the story of "Whitey" Bulger and The Winter Hill Gang is a legendary one. There are books and movies about this mobster from "Southie" (South Boston to those not in the know!). After on the lam for 16 years, Bulger was finally caught this week in southern California.

Whitey Bulger follows in similar footsteps of Jesse and Frank James, Bonnie and Clyde, and Butch Cassidy and The Sundance Kid - all notorious criminals that were hunted for a long time.

I have to admit, his arrest seems awfully anti-climactic - a quick and quiet arrest in his home, brought about by a tip from Iceland! Okay, so that tip sounds farfetched, but the details make sense.

So today, Whitey and his girlfriend are returned to South Boston to face arraignment, and sees his brother - a prominent Boston politician. And then he's whisked off to jail to await the next steps.

My guess is that this trial will take a very long time to complete. And, it's going to be an interesting one. Bulger is a very defiant character, and he's going to remain so throughout this trial. Stay tuned!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Sony Hacker Formally Charged!
""""""""""""""""""""""""""""""" Sonic the Hedgehog Hits 20!
"Duke Nukem" Is A Mess?!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

"""""""""""""""""""""""""""""""""""""

UK Hacker Formally Charged for Cyber Attacks

U.K. police on Wednesday formally charged a 19-year-old teenager with violating the country’s computer fraud laws for participating in cyber attacks on various British organizations.

Ryan Cleary violated the Criminal Law Act and Computer Misuse Act when he helped organize and carry out distributed denial of service (DDoS) attacks against the U.K.’s Serious Organised Crime Agency, the International Federation of the Phonographic Industry (IFPI), and the British Phonographic Industry (BPI), the Metropolitan Police said.

Cleary was arrested at his home in Essex yesterday; he will appear at the City of Westminster Magistrates Court on Thursday morning.

The 2010 attacks on the IFPI and BPI were reportedly orchestrated by Anonymous offshoot Operation Payback, while the joint Anonymous-LulzSec project known as Operation Anti-Security took credit for the SOCA hack, which happened just this week.

The SOCA Web site is hosted by an external provider and does not contain data from its investigations. Indeed, LulzSec and Anonymous did not post any info from the SOCA site.

Both groups, however, don’t appear to have any love for Cleary.

"Ryan Cleary is not part of LulzSec; we house one of our many legitimate chatrooms on his IRC server, but that’s it," LulzSec tweeted recently. "We use Ryan’s server, we also use Efnet, 2600, Rizon and AnonOps IRC servers. That doesn’t mean they’re all part of our group."

LulzSec is "at best, mildly associated" with Cleary, the group said.

Anonymous, meanwhile, got into a battle with Cleary several months ago. In May, the Italian arm of Anonymous said on its blog that Cleary, a "fellow helper," had compromised its network. In a May interview with UK publication Thinq_, Cleary claimed responsiblity for a DDoS on several Anonymous sites, and said he published the IP addresses of users visiting the site when he seized control.

Operation Anti-Security, meanwhile, is humming along. "We’re hoping to have Operation Anti-Security Payload #1 ready by Friday," LulzSec tweeted this afternoon.

Sonic the Hedgehog Gets Anniversary Bundle for 20th Birthday

The Blue Blur has left his teenage years. Today, Sega’s trademark character is celebrating his twentieth birthday.

In celebration, Sega is pushing the latest game in the series, Sonic Generations, and releasing a 20th anniversary bundle on the PlayStation Store.

The bundle, according to the EU PlayStation blog, includes the original Sonic the Hedgehog, Sonic 2, Sonic Adventure (and the DX Upgrade pack), Sonic 4: Episode 1, and a theme taken from the world of Sonic 4. It will be available for 20 days for $19.99.

Sonic Generations, meanwhile, is set to be released later this year, the game is a blend of old and new, featuring a throwback to the hedgehog's early years with 2D levels as well as 3D levels from later years.

PCMag software analyst Jeffrey Wilson had some game time with Sonic Generations back at E3. "It felt like a Sonic game should," he wrote, "Cartoony, fun, and fast. There are a handful of incredible camera shifts that show Sonic speeding through loops, launching over chasms, and bouncing off bumpers. The 2D levels are fast, but the 3D levels (where the camera is placed behind Sonic) feel even faster - almost too fast."

Sega has released an iOS app for the game, but unfortunately for most, it's only available in Japan. Andriasang, a Japanese gaming Web site, writes that the app has one stage (Sonic the Hedgehog 4: Episode 1), weekly wallpaper downloads, a mini-game dubbed "Sonic the Sketchhog," and a section with the latest Sonic news.

Today, you can download a Sonic Generations demo via the Xbox Live Marketplace or the PlayStation Network. The demo is only available for 20 days, and it gives players access to the series' most iconic environment, Green Hill. It will be playable in both classic 2D and stereoscopic 3D.

Sonic Generations will arrive November for the Xbox 360, PlayStation 3, and the Nintendo 3DS.

'Duke Nukem' An Ugly, Mean-Spirited Mess

There's a sequence in "Duke Nukem Forever" (2K Games, for the Xbox 360, PlayStation 3, $59.99; PC, $49.99) that's destined to be remembered as one of the all-time low points in the history of video games.

It takes place in the Hive, a sort of alien incubator. The Hive is filled with naked human women who have been abducted and impregnated by the aliens. When Duke - the "hero" - accidentally kills one of the women, he makes an extremely tasteless joke.

Duke eventually stumbles upon two women. They beg for their lives. Duke responds with an F-word-based pun and watches as the two women explode.

I'm not a squeamish person, but there's a point at which even the strongest stomach says enough is enough. Unfortunately, I had to keep playing "Duke Nukem Forever" - and while it never again reaches that low, there's nothing that justifies that level of sadism and misogyny.

You may be familiar with the long, strange history of "DNF." It had been in development since the mid-1990s - the adolescent years of the first-person shooter, before "Halo" and "Call of Duty." Last year, it was finally rescued from the scrapheap by Gearbox Software, the studio behind 2009's superb role-playing shooter "Borderlands."

What Gearbox has assembled is a mishmash of poorly paced, archaically

designed chunks of action. Along with the gunplay, "DNF" incorporates driving, running-and-jumping platform antics and even some rudimentary puzzle-solving, all of which would be welcome in a modern-day shooter if they were better executed. Instead, when you finally get to do something fun - like driving Duke's monster truck, the Mighty Foot - the game grinds to a halt by forcing you to stop and find gas.

The worst game issues are reserved for the excruciating boss battles. At the end of the Hive section, for example, you face off against the alien queen, who can only be taken down by high-powered ordnance. Every time you score a hit, though, she knocks you off your feet, so you have to hide from her while your "ego" (this game's equivalent of health points) recovers.

That's right: During one of the core battles in "DNF," the hero - established as the toughest, most fearless hero Earth has ever seen - spends most of the time hiding. And if Duke runs out of ego (which he will, often), you're subjected to a 30-second-plus loading screen. Pile up enough of those and you'll eventually decide the limited amount of "fun" you're having isn't worth the aggravation.

Survive the alien queen and you're treated to a pointless fetch quest in which you have to find three items in a strip club. Your reward? The creepiest lap dance ever.

All of which left me wondering: Who is Duke Nukem? The character was established in the '90s as a parody of two-fisted action heroes like Arnold Schwarzenegger and Jean-Claude Van Damme. But during Duke's decade-and-a-half in limbo, those targets became toothless, and the gags here about contemporary stars like Christian Bale and Justin Timberlake fall flat.

So in 2011, Duke is just a parody of his former self, spouting jokes that are either lifeless or sickening. At one point, the president of the United States tells Duke he's "a relic from a different era." I wish he had stayed there. No stars out of four.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

China Says No Cyber Warfare with U.S.

There is no cyber warfare taking place between China and the United States, a senior Chinese official said on Wednesday, after weeks of friction over accusations that China may have launched a string of Internet hacking attacks.

The two countries might suffer from cyber attacks, but they were in no way directed by either government, Vice Foreign Minister Cui Tiankai told a small group of foreign reporters ahead of a meeting with U.S.

officials in Hawaii this weekend.

"I want to clear something up: there are no contradictions between China and the United States" on the issue of hacking, Cui said.

"Though hackers attack the U.S. Internet and China's Internet, I believe they do not represent any country," he added.

Both countries were in fact already discussing the problem of hacking during their regular strategic consultations, Cui said.

"The international community ought to come up with some rules to prevent this misuse of advanced technology," he added.

State Department spokesman Mark Toner declined to comment on Cui's cyber-war comments, but said the inaugural U.S.-China Asia-Pacific Consultations in Honolulu had a general regional focus and no particular cyber warfare agenda.

"My understanding is that it is about the Asia-Pacific region, writ large," he said in Washington. Kurt Campbell, the assistant secretary of state for East Asian and Pacific affairs, would be Cui's counterpart in the talks, he said.

The accusations against China have centred on an intrusion into the security networks of Lockheed Martin Corp and other U.S. military contractors, as well as efforts to gain access to the Google email accounts of U.S. officials and Chinese human rights advocates.

China has vociferously denied having anything to do with hacking attacks, saying it too is a major victim.

"Internet security is an issue for all countries, and it is a most pressing matter," Cui said.

"Of course, every country has different abilities when it comes to this problem," he added.

"The United States is the most advanced country in the world when it comes to this technology, and we hope they can step up communication and cooperation on this with other countries. We also hope this advanced technology is not used for destructive purposes."

The Internet has become a major bone of contention between Washington and Beijing.

This month, Defense Secretary Robert Gates said Washington was seriously concerned about cyber attacks and was prepared to use force against those it considered an act of war.

The latest friction over hacking could bring Internet policy back to the foreground of U.S.-China relations, reprising tension from last year when the Obama administration took up Google's complaints about hacking and censorship from China.

Google partly pulled out of China after that dispute. Since then, it has lost more share to rival Baidu Inc in China's Internet market.

China, with more than 450 million Internet users, exercises tight control and censorship over the Web at home, and has strengthened its

grip in recent months.

In February, overseas Chinese websites, inspired by anti-authoritarian uprisings across the Arab world, called for protests across China, raising Beijing’s alarm about dissent and prompting tightened restrictions over the Internet.

China already blocks major foreign social websites such as Facebook and Twitter.

Commerce Secretary Gary Locke, named by President Barack Obama as the next U.S. ambassador to China, said last week that the United States was looking into ways to craft trade countermeasures that treat curbs on Internet commerce as non-tariff barriers to trade.

Brazen, Publicity-seeking Hackers on Attack Spree

Can you be famous if no one knows your name? A new band of hackers is giving it its best shot, trumpeting its cyber-capers in an all-sirens-flashing publicity campaign.

Lulz Security has stolen mountains of personal data in a dozen different hacks, embarrassing law enforcement on both sides of the Atlantic while boasting about the stunts online.

The group, whose name draws on Internetspeak for "laughs," has about 270,000 followers on the messaging site Twitter. Although LulzSec has declined interview requests, it has laid out its prankster philosophy in "tweets" and press releases.

"Vigilantes? Nope. Cyber terrorists? Nope. We have no political motives - we do it for the lulz," the group said in a message sent shortly after it emerged in early May.

LulzSec’s Twitter mascot is a black-and-white cartoon dandy that looks like a cross between Mr. Peanut and The New Yorker magazine’s monocle man. Its rambling messages are peppered with references to YouTube sensation Rebecca Black, the Dungeons and Dragons role playing game and tongue-in-cheek conspiracy theory.

One of LulzSec’s victims says the group sets itself apart from the rest of the hacker underground with its posturing and bragging on Twitter.

"Most of the hacker groups that are pretty well known out there ... don’t really like to flaunt their findings. They’ll do it among their peers, but not typically the public," said Karim Hijazi, a security expert whose emails were ransacked by the hacking group last month.

LulzSec made its name by defacing the site of the U.S. Public Broadcasting Service, or PBS, with an article claiming that rapper Tupac Shakur was still alive. It has since claimed hacks on major entertainment companies, FBI partner organizations, a pornography website and the Arizona Department of Public Safety, whose documents were leaked to the Web late Thursday.

Many attacks have yielded sensitive information including usernames and passwords - nearly 38,000 of them, in the case of Sony Pictures. Others

appear to have been just for kicks. In a stunt last week, LulzSec directed hundreds of telephone calls to the customer service line of Magnets.com, a New Jersey-based manufacturer of custom refrigerator magnets.

LulzSec uses a similar technique to temporarily bring down websites, flooding them with bogus Internet traffic. This is an old hacker standby that doesn't require much sophistication. Members also break in to sites to steal data. That requires more skill and often involves duping employees into revealing passwords.

LulzSec's actions against government and corporate websites are reminiscent of those taken by the much larger, more amorphous group known as Anonymous. That group has launched Internet campaigns against the music industry, the Church of Scientology, and Middle Eastern dictatorships, among others.

Both are fiercely protective of the secret-busting site WikiLeaks. The hacking groups' supporters share the same brand of offbeat humor inspired by Internet catchphrases and viral videos.

LulzSec has repeatedly insisted on its independence.

"We're not AnonOps, Anonymous, a splinter group of Anonymous, or even an affiliate of Anonymous," the group has said. "We're LulzSec."

An Anonymous member told The Associated Press that he believed LulzSec was formed by people from Anonymous who got tired of the time it took to reach consensus and launch hacking projects. He said that they also wanted to go beyond the ethical boundaries of Anonymous.

"They wanted to go on more adventurous, brazen hacking adventures and really get their names out there," he said. He spoke on condition that his name is withheld given the pressure being put on Anonymous members by law enforcement.

Judging by the timing of its tweets and other communications, he believes that LulzSec is based mainly in the eastern half of the U.S., but a few members are European. The number of members is not known, but there appears to be no more than a handful, perhaps a dozen.

Anonymous also uses Twitter as a soapbox, but more as a way of recruiting helpers than publicizing its exploits. It's also been more selective about its targets. It attacked the Egyptian Ministry of Information's website during the revolution in the country, but has shied away from leaks of ordinary user information, for example.

There's every sign authorities are paying attention to the new group, although it isn't clear how much progress they've made in tracking the hackers down. On Tuesday, 19-year-old Ryan Cleary was arrested as part of a joint FBI-Scotland Yard investigation into hackings linked to both LulzSec and Anonymous.

British Police Commissioner Paul Stephenson described Cleary's arrest as "very significant," although LulzSec has shrugged off the development - and promised more spectacular hacks.

The Anonymous member believes law enforcement has little chance of finding LulzSec. He told the AP that LulzSec likely used such methods as logging on only from public Wi-Fi hotspots. Police could possibly trace

the attacks to the hotspot, but by the time they get there, any hacker would be long gone.

Hijazi believes LulzSec harassed him because his firm, Unveillance, tracks "botnets" - clusters of computers that can be controlled remotely because they've been infected with malicious software. The botnets, each of which can have more than a million computers, are usually controlled by cybercrime gangs.

He speculates that LulzSec wants botnets because it would boost its power to bring down websites. But the group would be stepping on the toes of some very dangerous people if members started taking over botnets, he said.

"It's going to make everyone really mad, both the good guys and some really big bad guys," he said. "I hope law enforcement finds them first."

FBI Targets Two "Scareware" Rings in U.S., Europe

Police in the United States and seven other countries seized computers and servers used to run a "scareware" scheme that has netted more than $72 million from victims tricked into buying fake anti-virus software.

Twenty-two computers and servers were seized in the United States and 25 others in France, Germany, Latvia, Lithuania, the Netherlands, Sweden and the United Kingdom, the U.S. Justice Department said in a statement on Wednesday.

The suspects involved in the scheme, who were not identified, planted "scareware" on the computers of 960,000 victims. The scareware would pretend to find malicious software on a computer. The goal is to persuade the victim to voluntarily hand over credit card information, paying to resolve a nonexistent problem.

Latvian authorities seized at least five bank accounts believed to have been used by the leaders of the scam, and the Justice Department said nothing about arrests.

U.S. authorities also said on Wednesday they disrupted a second scam, charging two Latvians with running a similar scareware scheme that led to $2 million in losses through an advertisement placed on a Minnesota newspaper's website.

Peteris Sahurovs, 22, and Marina Maslobojeva, 23, were arrested on Tuesday in Latvia and face two counts of wire fraud, one count of conspiracy and one count of computer fraud in the United States, the Justice Department said.

"Scareware is just another tactic that cyber criminals are using to take money from citizens and businesses around the world," said Assistant Director Gordon Snow of the FBI's cyber division.

Law enforcement officials would not confirm whether the seizures were directly connected to a raid early on Tuesday morning at a web-hosting company in northern Virginia where they took servers, a move that disrupted more than 120 websites.

U.S. authorities have been more aggressive this year in trying to stem cybercrime and have been scrambling to investigate several hacking attempts on U.S. institutions and corporations.

In March, law enforcement raided servers used by a "botnet," essentially computers controlled by criminals without the knowledge of the computers' owners. Authorities severed the IP addresses, effectively disabling the botnet.

That operation, nicknamed Rustock, had been one of the biggest producers of spam e-mail, with some tech security experts estimating it produced half the spam that fills people's junk mail bins.

In April, government programmers shut down a botnet which controlled more than 2 million PCs around the world to spread a computer virus named Coreflood, which grabbed banking credentials and other sensitive financial data. Losses were estimated at about $100 million.

A botnet is essentially one or more servers that spread malicious software and use the software to send spam or to steal personal information or data that can be used to empty a victim's bank account.

Pentagon to Prep for Battle Via 'National Cyber Range'

In recent months, groups like LulzSec have shown that no one is safe from cyber attacks. In an effort to help individuals ward off Web-based threats in the U.S., the Pentagon's Defense Advanced Research Projects Agency (DARPA) is developing a virtual firing range that could be online as soon as next year, Reuters reports.

The program, dubbed National Cyber Range, will be a sandbox for virtual warriors to hone their skills. According to Reuters, it will be operational by mid-2012 - to the tune of $130 million.

The National Cyber Range has been in the works since 2008, when the Pentagon approached contractors to build the program. In January 2009, Lockheed Martin, itself a recent cyber-attack victim, was awarded a $5.4 million contract for the initial development of the National Cyber Range. The company was then awarded $30.8 million in February 2010 for phase two.

The National Cyber Range will be a collection of "testbeds" that can be used for standalone drills or as parts of larger operations. Reuters said one of the major aims of the NCR is to run multiple classified and unclassified experiments very quickly, requiring a system that can delete data and reboot as fast as possible after a test.

Reuters pointed to two other cyber-related programs DARPA has in the works: Clean-slate Design of Resilient, Adaptive, Secure Hosts (CRASH and Cyber Insider Threat (CINDER).

CRASH is focused on designing new computer systems that are resistant to cyber attacks and can adapt over time, while CINDER is focused on detecting espionage hidden on computer networks. CINDER evolved out of last year's WikiLeaks scandal in which Army analyst Bradley Manning was arrested for giving information to the whistleblower Web site.

DARPA is also developing the "Cyber Genome" which will be able to automatically discover, identify, and analyze malicious code which can help identify the perpetrator, Reuters said.

Hackers Might Face Stiffer Sentences in U.S.

Even before a loosely organized group of hackers broke into the CIA's and Senate's public websites, the White House asked for stiffer sentences for breaking into government and private computer networks.

Last month the Obama administration pressed Congress to pass stronger cybersecurity measures, including a doubling of the maximum sentence for potentially endangering national security to 20 years in prison.

While it remains to be seen if the proposal will become law, the question of how to fight cyber-crime has risen to the fore in recent weeks with a spate of high-profile, and sometimes, sophisticated, attacks.

The computer break-ins have targeted multinational companies and institutions, including Sony Corp, Citigroup and the International Monetary Fund. Sony faces dozens of lawsuits related to the theft of consumer data from its Playstation network.

Also, in the latest flurry of hack-ins, the loosely organized group Lulz Security said it broke into the Senate's and CIA's public websites, as well as Sony and other targets.

"It's been a busy month," said James Lewis, of the Center for Strategic and International Studies think tank.

Lewis said "hacktivists," who often break into websites to make a political point or generate publicity, made "a big mistake" in going after the public websites of the FBI and the CIA. "That bumps it up immediately," he said. "That could make it a grudge match."

But tackling cybercrime - as well as other kinds of cyberattacks - has often been complicated by the difficulty of determining who is responsible.

"Smoking keyboards are hard to find," said Frank Cilluffo, director of George Washington University's Homeland Security Policy Institute.

"Anonymity of cyberspace, the lack of being able to do 100 percent attribution makes it difficult from a national security standpoint, obviously, if you don't know who is behind the clickety clack of the keyboard, or even if you do, you don't have 100 percent confidence," he said.

Under current law, for first-time offenders, the Computer Fraud and Abuse Act sets a maximum of 10-year prison sentences for breaking into a U.S. government computer if national security is at stake, a maximum of five years for breaking into a computer in order to steal, and one year for stealing a password to a financial institution or accessing a government computer, for example to deface it.

Under the White House proposal, the 10-year maximum sentence for potentially endangering national security would become a 20-year

maximum, the five-year sentence for computer thefts up to $5,000 would become a 10-year sentence and the one year maximum for accessing a government computer - either to deface it or download an unimportant file - could become a three-year sentence.

At this point, none of the cybersecurity legislation introduced or circulating in Congress have included those tougher sentences.

And Stephen Ryan, a former prosecutor, said that if the goal is deterring cybercrime, lengthy sentences won't do the trick as well as actual arrests and prosecutions.

"There may be people who fully deserve a sentence that's more than five years. The key to deterrence is prosecution and conviction," said Ryan, now a partner at McDermott, Will & Emery.

Catching sophisticated hackers is notoriously difficult, which often means the sloppy and the stupid will end up being prosecuted -- as well as a few who just have bad luck.

"There's also the question of resources," said a cyber expert who asked not to be named "So when you're talking about nuisances - like the Senate and CIA - a lot of this comes across as childish vandalism. In those cases you have to question whether you devote the resources and prosecute that."

But the sentences can get longer if other crimes are involved. Alberto Gonzalez was sentenced to 20 years in prison in 2010 for hack attacks into major U.S. companies that led to the theft of more than 40 million credit and debit card numbers.

PrivateSky Shields Online Exchanges from Prying Eyes

A free service launched on Wednesday called PrivateSky lets Internet users shield email, Facebook updates, and other online exchanges from hackers or other unwanted snoops.

The service from startup CertiVox comes as hackers appear to be rampaging through the Internet, cracking defenses at companies, attacking public websites, and tricking their way into email accounts to spy on contents.

PrivateSky works with Internet Explorer (IE) browsers to provide encryption for whatever people type into message boxes and decodes it only for those they chose.

Users highlight blog posts, Facebook updates, email messages or other text then indicate who should be allowed to read them. Missives are decrypted only for intended recipients.

"It is literally one click encryption and decryption," said CertiVox founder and chief executive Brian Spector.

Internet security firm Trend Micro warned this month that cyberattackers have attempted to infiltrate Web-based email services run by Microsoft and Yahoo! as well as Google.

"There has been a variety of recent attacks on popular Webmail platforms," Trend Micro senior threat researcher Nart Villeneuve said in an online post. "In addition to Gmail, Hotmail and Yahoo! Mail have also been targeted."

Trend Micro released the news after Google said a cyber spying campaign originating in China had targeted Gmail accounts of US officials, military personnel, journalists, Chinese political activists, and officials in several Asian countries, mainly in South Korea.

Encrypting email is seen as a way to thwart email snooping, but the process has typically taken a bit of software savvy.

CertiVox set out to make encryption simple with PrivateSky. "This is kind of like arming the citizenry," Spector said.

The encryption service works on any Web-based email such as Gmail, Hotmail or Yahoo! Mail as well as posts at social networks.

CertiVox started with IE because of its global popularity but is adapting the service to other Web browsing software. CertiVox intends to eventually encrypt photos and other large data files as well as text.

The application for IE browsers is available for download online at https://privatesky.me.

Coming Soon to The Internet: The .whatever Address

A quarter-century after the creation of ".com," the agency that assigns Internet addresses is loosening its rules and allowing suffixes named after brands, hobbies, political causes and just about anything else.

Under guidelines approved Monday, Apple could register addresses ending in ".ipad," Citi and Chase could share ".bank" and environmental groups could go after ".eco." Japan could have ".com" in Japanese.

It’s the biggest change to the system of Internet addresses since it was created in 1984.

More than 300 suffixes are available today, but only a handful, such as the familiar ".net" and ".com," are open for general use worldwide. Hundreds of new suffixes could be established by late next year, thousands in years to come.

"This is the start of a whole new phase for the Internet," said Peter Dengate Thrush, chairman of the Internet Corporation for Assigned Names and Numbers, the California nonprofit organization in charge of Internet addresses.

The novelty addresses will be costly - $185,000 to apply and $25,000 a year to maintain one. A personal address with a common suffix such as ".com" usually costs less than $10 a year.

ICANN says it costs tens of millions of dollars to write the guidelines for suffixes, review applications and resolve any disputes. Even with the hefty fees, the organization says it plans only to break even. It’s also setting aside up to $2 million to subsidize applications from

developing countries.

The expansion plan, which runs about 350 pages, took six years to develop.

Before 1998, the United States, which paid for most of the early Internet, was in charge of handing out Internet suffixes. ICANN, which has board members from every inhabited continent, was a way to take the administrative burden off the U.S. government.

ICANN was always supposed to expand the number of available Web suffixes. But the progress was slow because of concerns that new ones could infringe on trademarks, be obscene or give a platform to hate groups. Competing interests wrestled with ICANN over guidelines.

ICANN has come up with procedures for any party to object to applications for trademark, or other reasons.

Internet addresses, technically known as domain names, tell computers where to find a website or send an email message. Without them, people would have to remember clunky strings of numbers such as "165.1.59.220" instead of "ap.org."

But the addresses have grown to mean much more. Amazon.com has built its brand on one, and bloggers take pride in running sites with their own domain names, uncluttered by the names of hosting services.

The address expansion could create new opportunities for companies to promote their brands and allow all sorts of niche communities to thrive online. But they could create confusion, too.

And they might not make much difference. More and more people online find what they’re looking for by typing a term into a search engine, not tapping out a full address. Or they use an app and don’t type anything.

ICANN will start taking applications for new suffixes Jan. 12. Approval of individual applications is expected to be quick if there are no challenges for trademark, morality or other reasons. Proposals that are challenged would have to undergo more thorough reviews, including possible arbitration to decide on the merits of claims.

High-profile entertainment, consumer-goods and financial-services companies will likely be among the first to apply for the new suffixes to protect their brands.

Canon Inc., the camera and printer company, already plans to apply for ".canon." And Apple could go after not just ".apple," but also ".ipad" and ".iphone." Apple had no comment Monday.

Groups have already formed to back ".sport" for sporting sites, and two conservationist groups separately are seeking the right to operate an ".eco" suffix. Trade groups for bankers and financial-services companies are jointly exploring applications for ".bank," ".insure" and ".invest" for their member companies.

Smaller companies stand to benefit, too. A florist called Apple can’t use "Apple.com" because the computer company has it. Previously, the shop might have registered a longer, clunky address. Now it can just be "Apple.flowers."

Of course, a small florist might not be able to afford an expensive

suffix. But an entrepreneur or a trade group might, and it could sell individual addresses ending in ".flowers" for $10 or $100 a pop. A successful suffix owner could make millions, much more than what it pays in application and annual fees.

When two or more groups have a legitimate claim to an address, ICANN expects them to work it out on their own. If they can’t, the nonprofit will auction the suffixes.

"Things are going to have to be decided, like ’Who’s a better guardian for .golf?’ The PGA or some global group?" said Jeremiah Johnston, chief operating officer at Sedo.com, which helps companies resell domain names.

Sedo brokered the sale of Sex.com late last year for $13 million, a record for a domain name. Despite the availability of new suffixes, Johnston doesn’t expect the value of existing ".com" names to diminish. That’s based on the limited number of additions to the system since 2000.

"Even though the new extensions come around, the ones that are most rooted and most popular in the minds of consumers, their value has only gone up," Johnston said.

Twins Drop Facebook Lawsuit Detailed in Hit Movie

The Harvard University classmates of Facebook founderMark Zuckerberg are ending the legal battle made famous by the Hollywood movie "The Social Network."

In a one-paragraph court filing Wednesday, Cameron and Tyler Winklevoss said they would accept a settlement that was worth $65 million when agreed upon in 2008.

The twins had sought to undo the settlement of $20 million cash and $45 million in stock.

The 9th U.S. Circuit Court of Appeals ruled against the twins, saying they had been represented by a squadron of Silicon Valley lawyers and their father, a noted business professor.

The twins said Wednesday they would forgo a trip to the U.S. Supreme Court.

Their stock is now worth more than $100 million.

Firefox 5 Begins Auto-Updates, Ends Firefox 4 Support

Mozilla released a new Firefox browser Tuesday as the first fruit of its commitment to a new fast-track process under which the browser will be automatically refreshed at eight-week intervals. The vast majority of the Firefox 5 improvements are under the hood, including support for the CSS Animations standard and a new privacy feature that lets users opt out of tracking used for behavioral advertising.

Unlike previous Firefox releases, the launch of Firefox 5 came without

huge fanfare. But with the rollout, the Mozilla Foundation is also ending security updates for Firefox 4, which received its final scheduled patch in April.

"Firefox 5 will be the security update for Firefox 4 and delivered as a minor update," wrote Firefox release manager Christian Legnitto late last month in a Mozilla developer mail list. "We most definitely reserve the right to change the plan later due to new information or invalid assumptions, but we are currently driving to mark Firefox 4 as unsupported when Firefox 5 comes out."

Some Firefox 4 users may not want to click on the upgrade to Firefox 5 pop-up window when it appears because of concerns about the new version’s compatibility with the plug-ins they are currently using. If they delay updating or opt out of the process entirely, however, this will leave them vulnerable to security holes.

On the other hand, Mozilla left the door open should a critical security flaw arise in Firefox 4 that requires immediate attention. "But that would be an ’unplanned’ emergency release and not a planned one," wrote Asa Dotzler, community coordinator for Firefox marketing projects.

Mozilla intends to treat Firefox 3.6 users differently from Firefox 4 users "because the jump from 3.6 to 4 is much larger than the jump from 4.0 to 5.0," Dotzler wrote. The goal is to "keep supporting 3.6 with security updates and increasingly loud prompted updates to our latest release until that number of users is low enough to make the updates automatic."

Firefox held 21.74 percent of the global browser market at the end of May, according to Net Applications, and its market share has hovered around 22 percent for the past year. According to the web-metrics firm, Firefox 4 had a 10.08 percent share last month, with Firefox 3.6 holding 9.14 percent.

Microsoft has already moved the majority of its Internet Explorer users worldwide to IE8, which held 31.28 percent of the market in May, according to Net Applications. But the software giant’s latest IE9 offering has yet to gain much market traction with a tiny 4.19 percent share. Additionally, 7.04 percent of all browser users worldwide were still running IE7 at the end of May, and 10.36 percent were using IE6.

Mozilla’s goal is to make each future browser release a nonevent for users like Google’s Chrome browser.

"Mozilla’s shift to a rapid-release development cycle delivers cutting-edge Firefox features, performance enhancements, security updates, and stability improvements to users faster," a Mozilla blog explained. "The latest version of Firefox includes more than 1,000 improvements and performance enhancements that make it easier to discover and use all of the innovative features in Firefox."

Opera Lightens Its Desktop Web Browser

Opera, the Nordic company that makes the Web browser of the same name, today teased a roadmap of improvements to its product, called Project Featherweight, aimed at making the browser lighter and faster.

Jan Henrick Helmers, a user-experience and graphics specialist at the company, posted today on Opera's blog the news that phase one of Project Featherweight, which aims at making the browser "as light, bright, and user-friendly as possible - without sacrificing power or flexibility," has been completed and released. "We want the user interface to match the speed of our rendering engine," Helmers added.

Major changes that Opera users will notice right off the bat include a newly designed address bar and status bar, with brighter yet softer colors for background and borders. The toolbar icons have also been refreshed. Opera has done away with the borders on buttons in the address bar and has made the Home and Fast Forward buttons optional. Mac users will see a new window gradient, too.

Although Helmers indicates that this rollout is "phase one" of the project, he did not mention what other improvements will follow.

Project Featherweight comes on the heels of yesterday's news from Mozilla announcing the availability of Firefox 5.0, which some users griped was a bit of a numbers game, considering version 4.0 was made public just three months ago.

Opera has been on the market since the mid 1990s. It gained popularity outside of the United States, notably in the Ukraine, because it offered support for some non-English language characters much earlier than other browsers. Opera's mobile browser, Opera Mini, is reportedly the most downloaded of all mobile browsers. The improvements seen in this first phase of Project Featherweight appear to only apply to the desktop version of the product.

DuckDuckGo: The Privacy-centric Alternative to Google

Remember when Altavista was the search engine? Or Yahoo? They stuffed their search pages with useless, distracting crap, and using them became unpleasant. And then, bam, along came Google, with a simple, clear search page and uncluttered search results. However, now that Google has become this massive behemoth, tracking our every move, and tailoring our search results, leading to only being fed those pages you agree with - isn't it time for something new? Something simple? It might be, and you've undoubtedly heard of them: DuckDuckGo. I'm switching. Update: Just got an email from Gabriel Weinberg, the guy behind DuckDuckGo. The OSNews !bang (!osnews) is now live!

DuckDuckGo is a relatively new search engine that has really been gaining in popularity recently. On OSNews alone several people regularly advise others to try it out whenever we talk about online privacy. So, what are some of the reasons you might want to try out DuckDuckGo?

First of all, DuckDuckGo doesn't track you, so you get real privacy when you search the web. Google tracks pretty much everything you do so they can better target you with advertisements. I have no problems with targeted advertising, and I have no issues in and of itself with Google collecting such information (in the end, I decide what I feed the web).

What does bother me, though, is the fact that I wouldn't be able to protect myself if the US government ever subpoena'd Google to gain access to that

information. Of course, I am of no interest to them (even my porn habits are incredibly boring), but it's the principle of the thing. Mind you that this is not mindless US-bashing; the same concerns apply to my own government and the EU. However, at least here in The Netherlands or even the EU I would have some means to defend myself against such government behaviour - I don't in the US.

That's why I love the idea of a search engine that doesn't track me. God knows, I might develop some embarrassing illness in the future, and I would rather keep something like that under wraps. DuckDuckGo is the answer here - no tracking, no information sharing. DuckDuckGo doesn't send your search terms to the web sites you visit. It also has various other privacy features, such as the ability to use POST requests, HTTPS with the ability to automatically force sites in the search results to also use HTTPS, and integrated Tor functionality, so you can get completely end-to-end anonymous and encrypted search.

More importantly though (at least for me) - DuckDuckGo tries to pop something called the filter bubble. "A filter bubble is a concept developed by internet activist Eli Pariser to describe a phenomenon in which search queries on sites such as Google or Facebook or Yahoo selectively guess what information a user would like to see based on the user's past search history and, as a result, searches tend to play back information which agrees with the user's past viewpoint," Wikipedia summarises, "Accordingly, users get less exposure to conflicting viewpoints." In the below TED talk, Pariser explains it in more detail.

So, is this all, or are there any other reasons to try DuckDuckGo? Well, I really like the !bang syntax, which allows for all kinds of CLI-like commands to be parsed to DuckDuckGo. Of course, things like !youtube query work, but also something like !safeoff query to perform a single search without safe search on. The list of !bangs is pretty extensive already, and yes, I've sent them a request to have !osnews turned into a !bang, too.

Other interesting goodies are listed on the, uh, goodies page. Of course, there are several browser extensions and smartphone applications for DuckDuckGo as well.

DuckDuckGo isn't perfect, obviously. It doesn't do image search, for instance (although you can use the !gi !bang for that), and more annoyingly, it's kind of a hassle to switch 'locales'. With Google, when I need to perform a Dutch search, I simply go to Google.nl and search from there; for international searches, I go to Google.com. With DuckDuckGo, I'd have to change locales in the settings page - as a translator, that's incredibly annoying. I might shoot them an email and ask if locale-switching could be done using !bangs (e.g. !nl query).

I'm starting the process of switching over to DuckDuckGo; it's now my default search engine in Chrome. It'll take a little getting used to, but then, I once switched from Altavista to Google without much hassle, so this should work too. Competition is good, and boy, does Google need it.

Final Snow Leopard Update Paves Way for Mac OS X Lion

Apple has rolled out the final update for the version of Mac OS X known as Snow Leopard. The 10.6.8 release is designed to pave the way for the launch of Mac OS X Lion next month as well as deliver a number of

critical bug fixes for Mac stability and security.

Initially released in August 2009, Snow Leopard was primarily dedicated to improving the performance and efficiency of Macs while reducing its memory footprint. However, Snow Leopard didn't offer much in the way of revolutionary new features. Mac OS X Lion promises to be different in this respect.

Before Mac users can download Lion, however, they must first upgrade to Snow Leopard 10.6.8, which has been specifically modified to make it possible for Mac users to download the next generation Mac OS exclusively from Apple's Mac App Store for $29.95. "By Apple having its Mac user base running upgraded software, [this] will expose the Mac base to new features, and increase the likelihood they remain on Mac," noted Piper Jaffray analysts Gene Munster and Andrew Murphy.

Apple's final Snow Leopard update includes security fixes to combat new variants of a pernicious scareware program that masquerades as legitimate security software. According to Apple, Snow Leopard 10.6.8 is able to identify and remove all known variants of the bogus Mac Defender, which attempts to trick Mac users by pretending to detect nonexistent viruses that the victim can remove by purchasing the "full version" of the fake program with credit cards.

Apple released a Snow Leopard update at the end of May that was supposed to discover and remove the Trojan program from infected Macs. However, the cybercriminals behind the scam quickly unleashed immune variants that continue to be a threat. With the 10.6.8 update, Apple hopes to shut down the bogus Mac Defender for good. "Altogether, 40 bugs are fixed in this update," according to security software firm Intego.

For example, Snow Leopard 10.6.8 slams the door on the ability of maliciously crafted fonts embedded into documents to wreak havoc on Mac machines. And users will no longer be susceptible to images with an embedded ColorSync profile that were maliciously crafted, or have to worry about someone with a privileged network position being able to intercept their credentials or other sensitive information.

Apple's final Snow Leopard update contains improved support for IPv6 - the next-generation Internet Protocol slated to replace succeed IPv4, which is close to its ceiling of approximately 4.3 billion Internet addresses. Apple also said the update will improve the reliability of virtual private network (VPN) connections.

Still, Apple's 474MB Snow Leopard upgrade is primarily about rolling out the red carpet for Mac OS X Lion, which will bring many of the features of Apple iOS for mobile devices to the Mac platform. Among other things, Lion will feature an intelligently articulated "launchpad" display of the machine's installed apps as well as a new FileVault 2 program that automatically encrypts the machine's hard drive.

Lion is designed to run on newer Macs equipped with selected microprocessors from Intel, such as the Core 2 Duo, Core i3, i5 and i7, or one of the chipmaker's high-end Xeon chips. Other Lion requirements include a minimum of 2GB of memory and 4G of free disk space. Older Macs with PowerPC processors will not be able to upgrade to OS X Lion.

Penny Auction Sites Could Cost A Chunk of Change

An iPad for $88.07? An Xbox for $15.33? Sold!

The television commercials for online penny auctions may have viewers fantasizing about scoring the latest tech gadgets at eye-popping discounts. But they could be in store for a big letdown.

The issue is that penny auctions aren’t as straightforward as the name might sound. Unlike traditional auctions, participants have to pay to bid on an item. Every bid they place also adds more time to the auction clock. Those twists inject a gaming element into the shopping experience that some say confuses participants about how much they’re really spending.

"It’s not a typical auction where consumers can bid and pay only if they win," notes Becky Maier, a spokeswoman for the Better Business Bureau of Western Pennsylvania. "They’re paying to play."

One class-action lawsuit against a major penny auction site alleges the auctions are akin to a casino or lottery because the overwhelming majority of customers end up losing money.

The industry was virtually nonexistent just two years ago, but has grown to about 135 sites today, according to the research firm Technology Briefing Centers Inc.

The Better Business Bureau says penny auctions first came on its radar in 2009. The group issued consumer alerts on the sites shortly afterward as a result of an unusually high volume of complaints.

Before signing up for one of these sites, here’s what consumers need to know:

How They Work

To start bidding on an item, penny auction sites require users to buy a package of bids. Each bid typically costs 25 cents to $1, so a pack of 100 bids may cost $25 to $100.

The setup could make it seem like participants are only bidding a penny at a time, even though the bids actually cost much more. Every bid also puts another 10 seconds or so on the auction clock, meaning there’s a risk of getting caught up in the thrill of a bidding showdown.

To break down the economics of a sale, consider a flat-screen TV that ends with a winning bid of $100. If the final bidder placed 20 bids during the auction, the total cost would be $120 - $20 for the bids (assuming each bid costs $1) plus $100 for the TV.

Even after tacking on a shipping fee, that’s a steal and the winning bidder comes out looking like a shopping genius. But everyone else who took part in the auction is left lighter in the wallet with nothing to show for it.

"It’s only enjoyable if you win," says Zachary Schwartz, a 24-year-old from Markle, Ind.

Schwartz decided to give Beezid.com a try about a year ago. He started bidding on an iPad but quit after the price reached $100. He used up

about $80 in bids over the next few days without winning anything. He hasn’t gone on the site since.

Schwartz placed a complaint with the Better Business Bureau and ultimately received a refund from Beezid.com.

Another site, QuiBids.com, notes that it tries to soften the blow for disappointed bidders. The site has a "buy now" feature that lets users buy an item for its retail price. The amount they spent bidding is credited toward the purchase.

So how can the sites afford to give such steep discounts? Consider an item that sells for $100. Bidding starts at $0, so users would need to have placed 10,000 bids to drive up the price by a penny at a time. If a bid costs $1, the site would have raked in $10,000 on the sale. That’s not including the $100 the winner has to pay for the item.

Problems To Watch

The nature of the complaints received by the Better Business Bureau spotlights the potential pitfalls. Most commonly, consumers said they were automatically charged for free trials or that they couldn’t reach customer support. In other cases, consumers alleged that the sites used automated programs to drive up bid prices. So before signing up for an account, check with the BBB and research what users are saying about their experiences online.

It’s also a good idea to carefully read a site’s terms and conditions and understand the return policy. Also pay attention to whether there are any upfront fees.

Seb Clements, a 25-year-old who lives in Fort Worth, Texas, says he signed up for SwipeBids.com last year to do some Christmas shopping. The site requested his credit card information as part of the sign-up process. As soon as he hit the submit button, he received an email saying he’d been charged a $175 membership fee. The fee included 100 bids.

He immediately tried to dispute the charge but there wasn’t a phone number on the website. During an online chat with a customer service representative, he was told the money was not refundable.

"My wife and I ended up counting it as a life lesson," Clements says. The Federal Trade Commission last month took action against the operators of the site, alleging they swindled customers of $467 million through multiple online scams.

Tips on Playing

Despite the many concerns, the BBB notes that there are legitimate penny auction sites. Consumers who feel confident about giving it a try should keep a couple strategies in mind.

It’s important to be calculated about placing bids because each carries a price tag. So before jumping into an auction, observe the site for a few days. Check out the final sale prices and how long bidding typically lasts for different types of items.

Auctions typically start with 24 hours on the clock. Generally the bidding won’t begin in earnest until around the final 15 seconds, so it’s a waste to place bids any sooner. Because each bid puts more time

on the clock, the "final" 15 seconds will likely stretch on for some time.

It’s also good to get your feet wet with a small item. The competition won’t be as intense for a $15 gift card, for example, as for a flat-screen TV.

Publicity Stunt? Dating Website Dumps 30,000 ’Ugly’ People

Is this for real?

Dating website BeautifulPeople.com has reportedly removed more than 30,000 members from its site, claiming a virus allowed too many "ugly" people in last month.

Like the old college favorite HotOrNot.com, Beautiful People is a members-only site where its half a million members get to vote on who should be accepted, based purely on their looks. Applicants have 48 hours to be voted in by members of the opposite sex.

But in a curiously worded press release issued Monday, BeautifulPeople.com said its rating module had been attacked by the "Shrek" virus that let thousands of people bypass the voting process. As a result, it had to reject these members.

Greg Hodge, managing director of BeautifulPeople.com, told PCMag in an e-mail that the "Shrek" virus was time-activated to bring down the site’s rating system around the world. "It started in a few countries only, then moved on to the entire system until it completely took over the rating module," he wrote.

The virus has been contained and fixed internally, he said, and no existing member information was compromised. Most of the rejects came from the US, Canada, France, and Germany.

The company has also set up a "Removed Member Support Line" (1-800-791-0662) that connected to voicemail when we tried calling during its office hours.

Skeptical? So was Sophos Security’s Graham Cluely, who called the breach a "publicity stunt" in a blog post.

Cluely said the story was fishy because A) the company didn’t inform any other security firms about the malware, B) the virus didn’t compromise any private information of existing members, and C) the breach was contained and being investigated internally.

"So, lots of publicity for the website but nothing for current or future members to worry about then. How convenient!" Cluely wrote.

It wouldn’t be the first time the company has tried to trick the press. In 2009, BeautifulPeople.com launched an award-winning PR stunt by convincing media outlets that its members had to re-apply for membership after Christmas, if they had "let themselves go" during the holidays.

BeautifulPeople.com is headquarted in Los Angeles but its IT operations are based in Denmark.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.